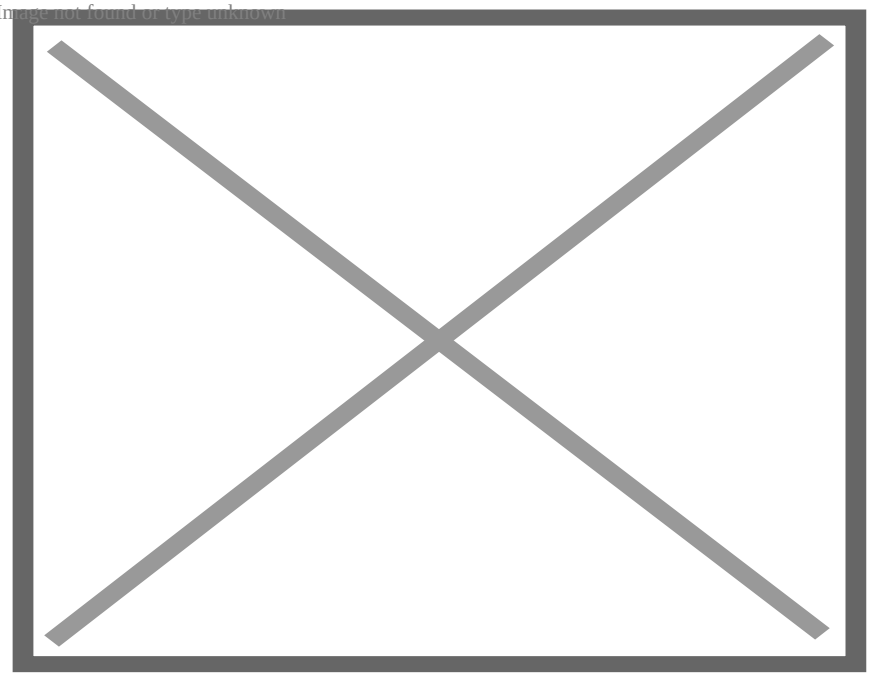
Secretly Copying Files To An External USB Drive

Description

Copying corporate data and using it at a competing company (intellectual property/corporate asset theft) is a common and serious concern for companies and their legal counsel. When employees leave companies, there are often questions about the security of the information they previously accessed. Will they use the contacts, forms, or product details as a competitive advantage in their new job?

I had previously written about using the file activity records in the index.dat file to identify when files were accessed. This can help determine if files were copied from a corporate file server. I want to expand on some additional artifacts that can be used and then provide an illustration. Three primary artifacts can help determine if someone accesses and copies specific files using an external drive, CD/DVD, flash device, or other storage media.

Image not found or type unknown



1) USBStor Registry Entry – Microsoft Windows uses its registry to track information about the computer's users, operating system, hardware, applications, security, and other relevant information. When USB devices are plugged into a computer, several key artifacts are captured, including the make, model, serial number (if available), drive letter, and when the device was plugged in.

2) Index.dat Access Record – Microsoft Windows uses the index.dat file to track website activity in Internet Explorer. It also contains when and from where files were accessed. We often have to recover deleted or purged activity using programs like NetAnalysis for thorough analysis. NetAnalysis can often

recover hundreds of thousands of records no longer available in the index.dat files on the system.

3) Link File (.lnk shortcut) – A user can create shortcuts commonly stored on the desktop. Microsoft Windows also automatically creates shortcuts for files accessed in .lnk files. These files store a wealth of information about the source document, including the path, date and time created, written, last accessed, size, volume serial, and several others. This information is encoded and requires special software to display it in a helpful format.

4) File Activity Logs – Newer versions of Windows, such as Windows 11, have more sophisticated features for tracking file activity, such as the new System Event Trace (SET) feature. SET can identify when a file was created, modified, or deleted. It can also show how a file was accessed (e.g., read, written, executed) and the application and device used to access it.

5) "File Sniper" – Use a product like Harvester from Pinpoint Labs to create a hash list of the suspect files and scan all locations where the files could be used. It isn't uncommon for a computer forensic examiner to be asked if there is a way to create a list of files from a corporate network or employee's system and check if a competitor uses them.

Using the above artifacts, it is possible to determine that files on a company server or client machine were copied or accessed after a specific date and time. Note that this doesn't provide the file's contents, and a thorough review would be necessary to ensure it is the same file. However, if the file name and other relevant metadata match, it does appear suspicious and may be enough to construct a solid argument that the employee did copy or burn files, access the contents, or use the information. This may lead to criminal and civil charges around possibly benefiting a future employer or a new company that the employee decided to start.

USB Artifacts Illustration (**Download PDF here**)

Date
11/27/2024
Date Created
11/21/2008